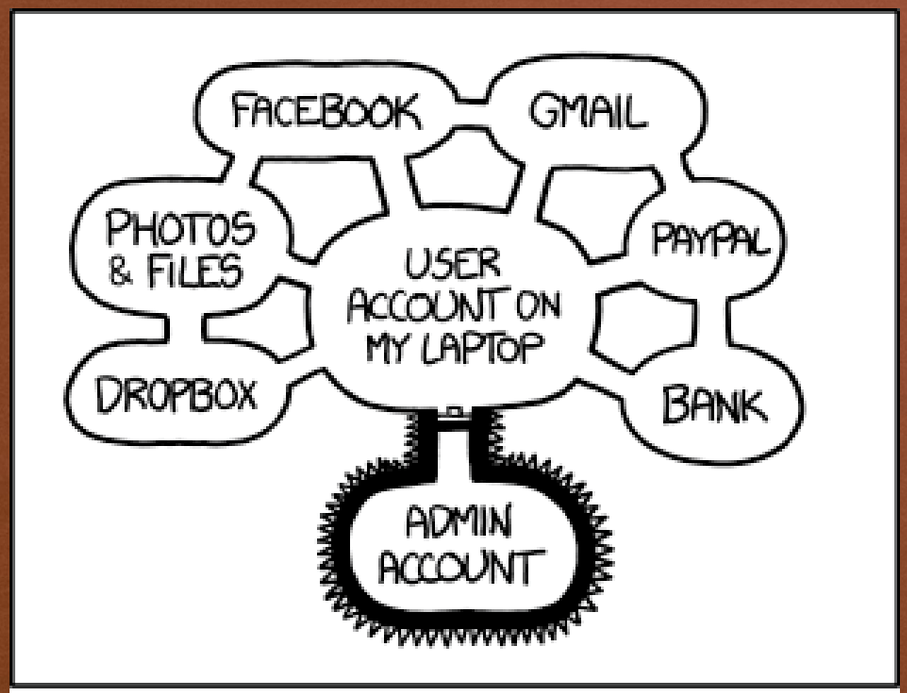
SECURITY

Chapter 8



IF SOMEONE STEALS MY LAPTOP WHILE I'M LOGGED IN, THEY CAN READ MY EMAIL, TAKE MY MONEY, AND IMPERSONATE ME TO MY FRIENDS,

BUT AT LEAST THEY CAN'T INSTALL DRIVERS WITHOUT MY PERMISSION.

https://xkcd.com/1200/

ENCRYPTION

- One of the risks that data is exposed to in storage or in transit between hosts is eavesdropping.

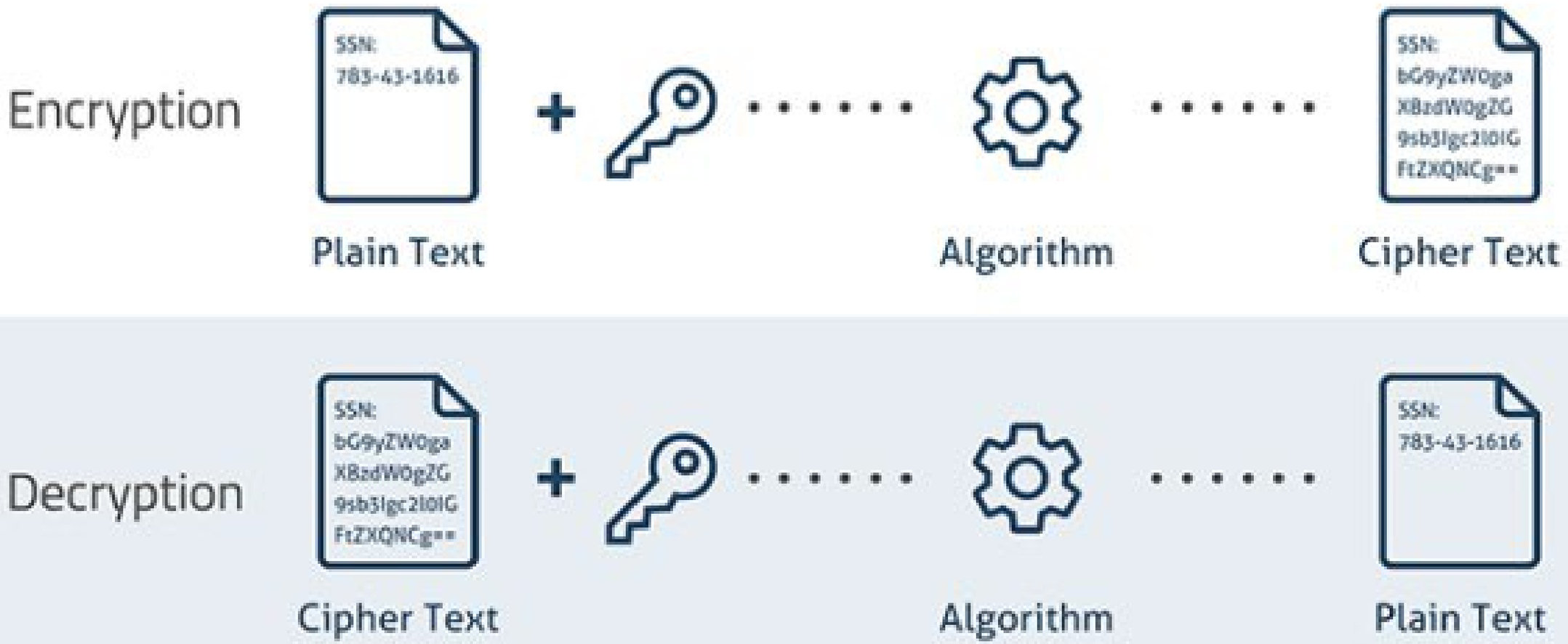
- **Encryption** and **decryption** (inverse operations)
  - Convert from plaintext to ciphertext and back again

- All encryption algorithms use a **key** of some kind to convert the plain text to cipher text.

- The intended recipient of the data uses the ciphertext and their key(s) to decrypt the encrypted data back to plaintext.

- **Cryptography**: science of “secret writing”

ENCRYPTION


Encryption
SSN:
783-43-1616
Plain Text
Algorithm
SSN:
bG9yZW0ga
XBzdW0gZG
9sb3Igc2l0IG
FtZXQNCg==
Cipher Text
Decryption
SSN:
bG9yZW0ga
XBzdW0gZG
9sb3Igc2l0IG
FtZXQNCg==
Cipher Text
Algorithm
SSN:
783-43-1616
Plain Text

SIMPLE ENCRYPTION ALGORITHMS

Caesar cipher (shift cipher)

- Map characters to others a fixed distance away in the alphabet
- Example, with a right shift of 5 letters:

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E

- **Stream cipher**: encode each character as it comes

- **Substitution cipher**: similar, but implement other mappings

- Pros: easy and fast, can do character by character
- Cons: letter frequency, double letters, easy to break (only 25 possible keys = 25 possible shift values)

Past question on encryption with a Caesar cipher

26. Consider the plaintext SOURSOP. If encrypted with a Caesar cipher with key 6, which of the following is the ciphertext? You may assume that the cipher's alphabet consists of the 26 letters of the English alphabet only.

A. YUAXYUL
B. YUAXYUV
C. YUAKLHI
D. YUAXMIJ
E. YUAXYJK

Plain	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
Cipher	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F

25. Consider a ciphertext XMAE. If you know that this was encrypted with a Caesar cipher from plaintext LAOS, which of the following could be the key? You may assume that the cipher's alphabet consists of the 26 letters of the English alphabet only.

A. 12
B. 21
C. 22
D. 15
E. 20

SIMPLE ENCRYPTION ALGORITHMS

Weakness of the Monoalphabetic Replacement Ciphers

- The cipher text maintains the “fingerprint” of the language.

- We can, therefore, use a “Frequency Analysis” table to decipher the text (given the text is long enough).

- Using frequency analysis to break a Caesar cipher text.

Try to decrypt a Caesar cipher code yourself: https://www.101computing.net/frequency-analysis/

https://www.youtube.com/watch?time_continue=2&v=sMOZf4GN3oc& feature=emb_logo

Past question on breaking a Caesar cipher

27. Decrypt the ciphertext `QCZZODGS`:

A. COLLAPSE
B. LIFETIME
C. ACCEPTED
D. HOMELESS
E. DATABASE

SIMPLE ENCRYPTION ALGORITHMS

Block cipher

- Block of plaintext encoded into a block of ciphertext.
- Each plaintext character in the block contributes to multiple cipher text characters.
- This destroys the structure of the plaintext making it hard to decrypt.

- Matrix-based block cipher
  - Group characters into blocks of “n” characters long.
  - Find invertible n by n matrix, M, and its inverse, M′ as keys -- this property is what allows M’ to **reverse the effect** of M.
  - Map characters to numbers A→1, B→2, etc.
  - Wrap values 26 and above back to zero: 26→0, 27→1, etc.

SIMPLE ENCRYPTION ALGORITHMS

Encryption Algorithm

Simple example: use a block size of 2.

Start with an encoding key, in this case a 2x2 matrix.

$$M = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix} \qquad M' = \begin{bmatrix} 23 & 5 \\ 2 & 23 \end{bmatrix}$$

Encrypt the plain text - "GO"

Step 1 : Convert plain text to a vector of numbers

$$\text{GO} \xrightarrow{\text{yields}} [6 \quad 14]$$

$$V = [6 \quad 14]$$

A = 0		N = 13	
B = 1		O = 14	
C = 2		P = 15	
D = 3		Q = 16	
E = 4		R = 17	
F = 5		S = 18	
G = 6		T = 19	
H = 7		U = 20	
I = 8		V = 21	
J = 9		W = 22	
K = 10		X = 23	
L = 11		Y = 24	
M = 12		Z = 25	

SIMPLE ENCRYPTION ALGORITHMS

Step 2 : Multiply the resulting vector with M, applying wraparound

$$V = [6 \quad 14] \qquad M' = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix}$$

$$[6 \quad 14] * \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix} = [6*3 + 14*2 \quad 6*5 + 14*3]$$

$$= [46 \quad 72] \bmod 26$$

$$= [20 \quad 20]$$

$[20 \quad 20]$ yields UU ← CipherText

A = 0	N = 13
B = 1	O = 14
C = 2	P = 15
D = 3	Q = 16
E = 4	R = 17
F = 5	S = 18
G = 6	T = 19
H = 7	U = 20
I = 8	V = 21
J = 9	W = 22
K = 10	X = 23
L = 11	Y = 24
M = 12	Z = 25

This **diffusion (scattering) of the plaintext** within the ciphertext is the **advantage** of a block cipher

SIMPLE ENCRYPTION ALGORITHMS

Decryption Algorithm

$$M = \begin{bmatrix} 3 & 5 \\ 2 & 3 \end{bmatrix}$$

$$M' = \begin{bmatrix} 23 & 5 \\ 2 & 23 \end{bmatrix}$$

Decrypt the cipher text UU

Step 1 : Map the cipher text to a vector of numbers

$$\text{UU} \xrightarrow{\text{yields}} [20 \quad 20]$$

$$V = [20 \quad 20]$$

A = 0		N = 13	
B = 1		O = 14	
C = 2		P = 15	
D = 3		Q = 16	
E = 4		R = 17	
F = 5		S = 18	
G = 6		T = 19	
H = 7		U = 20	
I = 8		V = 21	
J = 9		W = 22	
K = 10		X = 23	
L = 11		Y = 24	
M = 12		Z = 25	

SIMPLE ENCRYPTION ALGORITHMS

Example: Multiply the vector with matrix M

Step 2 : Multiply the resulting vector with M, applying wraparound

$$V = [20 \quad 20] \qquad M' = \begin{bmatrix} 23 & 5 \\ 2 & 23 \end{bmatrix}$$

$$[20 \quad 20] * \begin{bmatrix} 23 & 5 \\ 2 & 23 \end{bmatrix} = [23 * 20 + 2 * 20 \quad 20 * 5 + 20 * 23]$$

$$= [500 \quad 560] \bmod 26$$

$$= [6 \quad 14]$$

$[6 \quad 14]$ yields GO ← Plain Text

A = 0		N = 13	
B = 1		O = 14	
C = 2		P = 15	
D = 3		Q = 16	
E = 4		R = 17	
F = 5		S = 18	
G = 6		T = 19	
H = 7		U = 20	
I = 8		V = 21	
J = 9		W = 22	
K = 10		X = 23	
L = 11		Y = 24	
M = 12		Z = 25	

Past question on Encryption with a Block Cipher

28. Consider the plaintext FCG over the shortened alphabet A=0, B=1, C=2, D=3, E=4, F=5, G=6, H=7. What is the ciphertext if we encrypted the plaintext with the following block cipher key:

$$\begin{bmatrix} 7 & 5 & 1 \\ 1 & 0 & 2 \\ 4 & 1 & 7 \end{bmatrix}$$

Note: Given the size of the alphabet, you will need to use `mod 8`.

A. DAC
B. EEE
C. CCC
D. FHD
E. GAA

$$[5\ \ 2\ \ 6] * \begin{bmatrix} 7 & 5 & 1 \\ 1 & 0 & 2 \\ 4 & 1 & 7 \end{bmatrix} = [5*7+2*1+6*4 \quad 5*5+2*0+6*1 \quad 5*1+2*2+6*7]$$

$$= [61\ \ 31\ \ 51] \bmod 8$$

$$= [5\ \ 7\ \ 3]$$

SIMPLE ENCRYPTION ALGORITHMS

Encoding

1. Apply S mapping to plaintext block.
2. Multiply result times M, applying wraparound.
3. Apply S’ to the result.

Decoding

1. Apply S mapping to ciphertext block.
2. Multiply result times M’, applying wraparound.
3. Apply S’ to the result.

Steps in encoding and decoding for a block cipher.

ENCRYPTION

Types of Cryptographic systems – based on how the plaintext is processed

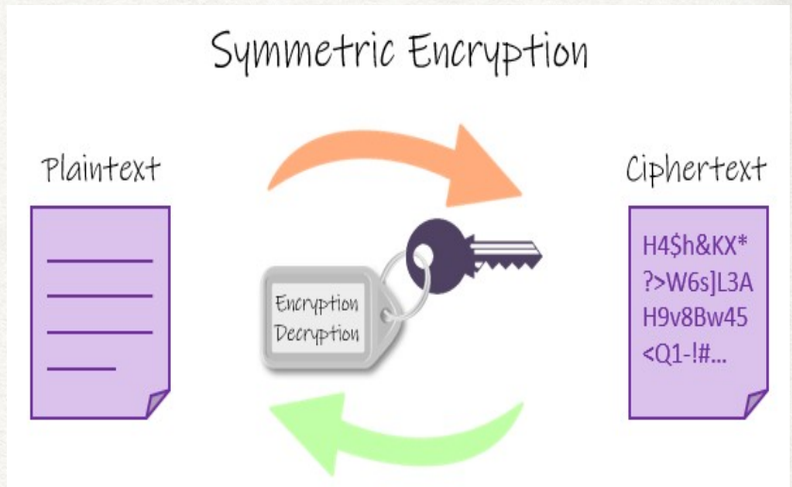
- **Block cipher**
  - processes the input one block at a time, producing an output block for each input block.

- **Stream cipher**
  - processes the input elements continuously, producing output one element at a time, as it goes along.

ENCRYPTION

Types of Cryptographic systems – based on the number of keys used.

- **Symmetric encryption algorithm**
  - A secret key shared by the sender and the receiver
  - Same key is used to encrypt and decrypt
  - Challenge – to securely transmit the secret key



- **Asymmetric encryption algorithm (public key encryption)**
  - Uses two keys: public and private
  - Use public key (generally known) to encrypt
  - Use private key (known only to receiver) to decrypt